NONPROVISIONAL PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400
Facsimile: (703) 836-2787

Attorney Docket No.: 104135

Date: November 28, 2000

BOX PATENT APPLICATION

NONPROVISIONAL APPLICATION TRANSMITTAL
RULE §1.53(b)

Director of the U.S. Patent and Trademark Office
Washington, D.C. 20231

Sir:

Transmitted herewith for filing under 37 C.F.R. §1.53(b) is the nonprovisional patent application

For (Title): SYSTEMS AND METHODS FOR POLICY BASED PRINTING

By (Inventors): Teresa F. LUNT, Matthew K. FRANKLIN

☒ Formal drawings (Figs. 1-2; 2 sheets) are attached.
☒ A Declaration and Power of Attorney is filed herewith.
☒ An assignment of the invention to XEROX CORPORATION is filed herewith.
☒ An Information Disclosure Statement is filed herewith.
☐ A Preliminary Amendment is filed herewith.
☐ Please amend the specification by inserting before the first line the sentence --This nonprovisional application claims the benefit of U.S. Provisional Application No. _____, filed _____.--
☒ The filing fee is calculated below:

CLAIMS IN THE APPLICATION AFTER ENTRY OF
ANY PRELIMINARY AMENDMENT NOTED ABOVE

FOR:	NO. FILED	NO. EXTRA	RATE	FEE
BASIC FEE				$ 710
TOTAL CLAIMS	17- 20	= 0*	x 18	$ ------
INDEP CLAIMS	2 - 3	= 0*	x 80	$ ------
☐ MULTIPLE DEPENDENT CLAIMS PRESENTED			+ 270	$ ------
* If the difference is less than zero, enter "0".			TOTAL	$ 710

☒ Please charge Deposit Account No. 24-0037 in the amount of $710.00. Two duplicate copies of this sheet are enclosed.
☒ The Director is hereby authorized to charge any other fees that may be required to complete this filing, or to credit any overpayment, to Deposit Account No. 24-0037. Two duplicate copies of this sheet are attached.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

John P. Darling
Registration No. 44,482

JAO:JPD/cmm

Inventor Information

Inventor One Given Name::	Teresa F.
Family Name::	LUNT
Name Suffix::	
City of Residence::	Palo Alto
State or Prov. of Residence::	CA
Country of Residence::	U.S.A.
Inventor Two Given Name::	Matthew K.
Family Name::	FRANKLIN
Name Suffix::	
City of Residence::	Palo Alto
State or Prov. of Residence::	CA
Country of Residence::	U.S.A.
Inventor Three Given Name::	
Family Name::	
Name Suffix::	
City of Residence::	
State or Prov. of Residence::	
Country of Residence::	
Inventor Four Given Name::	
Family Name::	
Name Suffix::	
City of Residence::	
State or Prov. of Residence::	
Country of Residence::	
Inventor Five Given Name ::	
Family Name::	
Name Suffix::	
City of Residence::	
State or Prov. of Residence::	
Country of Residence::	

Correspondence Information

Name Line One::	Oliff & Berridge PLC
Address Line One::	P.O. Box 19928
City::	Alexandria
State or Province::	VA
Postal or Zip Code::	22320
Telephone::	(703) 836-6400
Fax::	(703) 836-2787
Electronic Mail::	commcenter@oliff.com

Application Information

Title Line One::	SYSTEMS AND METHODS FOR POLICY BASED
Title Line Two::	PRINTING
Title Line Three::	

Title Line Four::
Total Drawing Sheets:: 2
Docket Number:: 104135

Continuity Information

>This application is a::
Application One::
Filing Date::
Patent Number::
which is a::
>>Application Two::
Filing Date::
Patent Number::

Prior Foreign Applications

Foreign Application One::
Filing Date::
Country::
Priority Claimed::
Foreign Application Two::
Filing Date::
Country::
Priority Claimed::
Foreign Application Three::
Filing Date::
Country::
Priority Claimed::

SYSTEMS AND METHODS FOR POLICY BASED PRINTING

BACKGROUND OF THE INVENTION

1. Field of Invention

This invention relates to document forgery protection systems and methods.

2. Description of Related Art

Various techniques are known for detecting and/or deterring forgery of an original printed document. Document forgery includes both unauthorized alteration of the original document and unauthorized copying of the original document. Previously, watermarks have been applied to documents to detect and/or deter forgery. Watermarks are printed marks on a document that can be visually detected or detected using special equipment. Fragile watermarks are marks that appear in an original printed document but that will not appear in a copy of the original document made on a standard photocopier or will be detectably degraded in the resulting copy of the document.

Robust watermarks are marks in an original document that will be accurately reproduced on any copy of the original document made on an standard photocopier so that information contained in the watermark can be extracted from the copy. There are two types of robust watermarks that can be used. The first type of robust watermark is a mark that appears on both the original document and a copy. The second type of robust watermark is a mark that is present, but that is not readily visible, on the original document, but that becomes clearly visible on a copy of the original document. The second type of robust watermark is also known as an invisible robust watermark.

Forgery of an original document containing a fragile watermark by copying the original document is easily detected by the absence of the watermark on the copy of the original document. Forgery of an original document containing the first type of robust watermark is detected by extracting information contained in the robust mark. This information could identify a custodian of the original document and information relating to copy restrictions or other restrictions as to the use of the information in the original document. Forgery of an original document containing the second type of robust watermark is detected by the visible presence of the watermark on the copy of

the original document. For example, the information contained in the second type of robust watermark could be a banner that reads "This is a copy" or a similar warning.

SUMMARY OF THE INVENTION

This invention provides systems and methods for adding fragile and robust watermarks to an original document as it is printed.

This invention separately provides systems and methods for printing a document requiring forgery protection using a number of trusted printers.

This invention separately provides a series of trusted printers that together permit differing levels of forgery protection to be provided to a document to be printed.

In accordance with various exemplary embodiments of the systems and methods according to this invention, a family of trusted printers is managed to provide a range of different forgery detection and deterrence techniques. The protection requirements for an original document to be printed are determined by a trusted printing policy. The factors used to determine the protection requirements required for the original document to be printed include the value of the document being created, assumptions about the resources available to an adversary or attacker, such as a potential forger, and the cost of providing the protections to the original document to be printed.

When an original document requiring forgery protection is to be printed, the print job for that document is routed to a trusted printer that can print a watermark that includes copy evidence and/or tracing information necessary to obtain the required level of protection. Copy evidence is evidence that can be obtained through an inspection of a document that indicates whether that particular document is an unauthorized copy of an original document. Tracing information is information printed on a document that identifies the custodian(s) of the original document and restrictions on further copying that apply to the custodian(s) and to the original document. Other information may also be included in the tracing information that serves to more uniquely identify the original. The required copy evidence is applied to the printed document through the use of fragile watermarks or robust watermarks. The required tracing information is applied to the printed document through the use of robust watermarks. The parameters of the selected trusted printer are set by a print

management system to print the watermark(s), including the copy evidence and/or tracing information, appropriate to the required level of protection.

These and other features of the invention will be described in or are apparent from the following detailed description of various exemplary embodiments of systems and methods according to this invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Various exemplary embodiments of systems and methods according to this invention will be described with reference to the following drawings, wherein:

Fig. 1 is a schematic diagram illustrating a print management system according to this invention; and

Fig. 2 is a flowchart of a document forgery protection printing method according to an exemplary embodiment of this invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Fig. 1 is a schematic diagram illustrating a system for policy based printing. A network 100 includes at least one server 110 that controls a plurality of computers 121, 122 and 23. The server 110 also controls a family 130 of trusted printers 131-135. A trusted printer is a printer that is available only to authorized users of the network 100. The server 110 includes an operating system 111 that allows users of the network 100 to use various applications stored in the server 110 on the computers 121, 122 and 123. The applications may include, for example, word processing applications, spreadsheet applications, image scanning and/or processing applications, and/or database management applications. Authorized users of the computers 121, 122 and 23 can use the applications stored in the server 110 and controlled by the operating system 111 to create documents 140. The applications process images of the document 140 that can be viewed on the display units 151, 152 and 153 of the respective computers 121, 122 and 123.

The document 140 can be printed by entering a print command into one of the computers 121 or 122 or 123 and sending a print job to the server 110. The operating system 111 includes a print management system 112 that selects one of the family 130 of the trusted printers 131-135 that can provide a required level of protection for the document 140 to be printed. The print management system 112 includes a policy 113 that maps the document protection requirements to the specific security protection techniques available from the family 130 of the trusted printers 131-135.

The policy 113 determines the required protection level for the document 140 to be printed by collecting information about the value of the document 140 from the document creator or owner or from any other person authorized to print the document 140. The information may include assumptions about potential forgery and the cost necessary to provide a level of protection to detect and/or deter the potential forgery. The user may enter the information about the document 140 through a graphical user interface provided on one of the display units 151-153 of the particular computers 121-123 being used to print the document 140.

The print management system 112 may also allow the users to question each of the trusted printers 131-135 to determine what protection level each trusted printer 131-135 provides. The print management system 112 may also provide information to the user about which forgery techniques each protection level is able to detect and/or deter and the costs of using each protection level. Each computer 121-123 may be controlled by the print management system 112 and/or the operating system 111 to display to users the protection levels that may be applied to the document 140 to be printed.

Each document 140 to be printed may also have a security level embedded in it, attached to it or otherwise associated with it, that the print management system 112 can use to identify the specific combination of protection techniques needed to detect and/or deter potential forgery. The policy 113 is programmable and may be adapted to the particular requirements of the organization that operates, owns or uses the network 100. The policy 113 may be programmed to assign a protection level or levels for every authorized user of the network 100 or for every computer 121-123 of the network 100.

Every user of the network 100 may have an identification that is programmed into the policy 113. The identification may be a login password or user identification. Every document 140 printed by the user identified by the identification may have be assigned a specified protection level, a minimum protection level and/or a maximum protection level.

Every computer 121-123 of the network 100 may have an identification value. The computer identification values may be programmed into the policy 113. Every print job sent by the identified one of the computers 121-123 to the server 110 may have a specified protection level, a minimum protection level and/or a maximum

protection level. The policy 113 determines the protection requirements for the document 140 to be printed by identifying the user that enters the print command and/or the computer 121-123 that sends the print job.

The policy 113 may also conduct a search of the content of the document 140 to determine the required protection level. The search could be, for example, a keyword search or a keyphrase search of the document 40. The protection requirements of the document 140 could be dependent on the number of occurrences of various ones of the keywords or keyphrases.

The policy 113 determines the security requirements for the document 140 to be printed. For example, the policy 113 may determine that the document 140 to be printed requires protection against forgery by copying using a standard photocopier. Alternatively, the policy 113 may determine that the document 40 to be printed requires protection against scanning, image processing, and alteration of the contents of the document 140. Once the policy 113 determines the security requirements, the print management system 112 identifies the specific combination of protection techniques needed to meet these requirements. The print management system 112 then routes the print job to one of the trusted printers 131-135 that can apply the appropriate protections and sets the parameters in the selected printer to apply the appropriate protection techniques to the document 140. Examples of the protection levels that can be applied to the document 140 when it is printed, the forgery techniques that the protection levels protect against and the equipment necessary for creating the protection level and verifying the authenticity of a document are described in Table 1.

Table 1

Protection Levels	Technique(s)	Protects Against	Equipment Needed
Level 0	Fragile variable copy evident watermark.	Adversary with standard copier and toner or ink. Blank originals attack.	Standard color printer, or special toner or ink, or hyperacuity printer with inspector.
Level 1	Robust variable invisible copy evident watermark with tracing information.	Adversary who can remove copy evident watermarks from originals. Blank originals attack. Compromised tracing attack.	Standard color printer with special toner or ink.

Level 2	Fragile variable fluorescing invisible copy evident watermark to print page offset, with tracing information.	Weak protection against tampering. Blank originals attack.	Special toner or ink and standard highlight or color printer. Enhancements could include toner sensor or sensor to verify the presence of the copy-evident watermark. Fluorescent light to verify.
Level 3	Fragile variable fluorescing invisible copy evident watermark to print page offset, with tracing information, digitally signed and glyph encoded.	Adversary who can scan, image process, and print and who has access to the special toner or ink.	Special toner or ink and standard highlight or color printer. Enhancements could include toner sensor or sensor to verify the presence of the copy evident watermark. Fluorescent light and fluorescent scanner to verify.
Level 4	Fragile variable fluorescing invisible copy evident watermark to print random portions of the page, with tracing information, digitally signed and glyph encoded.	Adversary who can scan, image process, and print and who has the special toner or ink.	Special toner or ink and standard highlight or color printer. Enhancements could include toner sensor or sensors to verify the presence of the copy evident watermark. Fluorescent light and fluorescent scanner to verify.
Level 5	Robust variable fluorescing black copy evident watermark with tracing information.	Adversary with standard standard copier and toner or ink. Compromised tracing attack.	Fluorescing black toner or ink in a standard highlight or color printer. Fluorescent light to verify.
Level 6	Robust variable fluorescing black copy evident watermark with tracing information to print fixed portions of the page.	Adversary with standard copier and tone or ink. Detached toner attack. Blank originals attack.	Fluorescing black toner or ink in a standard highlight or color printer. Fluorescent light to verify.
Level 7	Robust variable fluorescing black copy evident watermark to print random portions of the page, with the random pattern specification encrypted and glyph encoded	Adversary with standard copier and toner or ink. Adversary with a scanner and image processor. Detached toner attack. Compromised tracing attack.	Fluorescing black toner or ink in a standard highlight or color printer. Fluorescent light to verify. Inspector to read and verify the glyph.

Level 8	Robust variable fluorescing black copy evident watermark to print content dependent portions of the page, with tracing information, encrypted and glyph encoded	Adversary who alters tracing information. Adversary with standard copier and ink. Adversary who can scan and image process. Detached toner or ink attack. Compromised tracing attack.	Fluorescing black toner in a standard highlight or color printer. Fluorescent light to verify. Inspector to read and verify the glyph.

Although Table 1 shows various watermarking techniques usable either alone or in combination to provide a specified level of protection to a document, it should be appreciated that the table is merely one exemplary embodiment of a policy 113. Other combinations of watermarking techniques may be provided to enable a greater range of protection levels. The protection levels, the techniques, the forgery methods that are protected against, and the equipment necessary to apply the techniques to a document to be printed and verify if a printed document is an original or a forgery are described in U.S. Application Serial No. _____(Attorney Docket Number 104136), incorporated herein by reference in its entirety.

As shown in Fig. 1, the trusted printer 131 can print documents having Level 0 protection, the trusted printer 132 can print documents requiring Level 1 protection, the trusted printer 133 can print documents requiring Level 0 through Level 4 protection, the trusted printer 134 can print documents requiring Level 4 through Level 8 protection and the trusted printer 135 can print documents requiring Level 7 and Level 8 protection.

Fig. 2 is a flowchart of one exemplary embodiment of a document forgery protection printing method according to this invention. Beginning in step S1000, control continues to step S1100, where a user creates a document that requires forgery protection. Then, in step S1200, the user enters a print command to print the document requiring forgery protection. Next, in Step S1300, information about the protection levels is displayed to the user. Control then continues to step S1400.

In Step S1400, information is collected about the value of the document requiring forgery protection. The information may include information or assumptions about potential forgery of the document requiring forgery protection and the cost of applying the various available protection techniques to the document requiring forgery protection. Next, in step S1500, the protection requirements of the document requiring forgery protection are determined based on a trusted printing

policy. The determined protection requirements for the document requiring forgery protection may indicate that this document requires protection against forgery from copying using a standard photocopier or that the document requiring forgery protection requires protection against forgery by scanning, image processing and altering of the contents of the document. Then, in step S1600, the protection level that provides the specific combination of protection techniques to meet the determined protection requirements is determined. Control then continues to step S1700.

In step S1700, a trusted printer that can apply the appropriate protection techniques to the document requiring forgery protection is selected based on the determined protection level. Then, in step S1800, the print job for the document requiring forgery protection is routed to the selected trusted printer. Next, in step S1900, the parameters in the selected trusted printer are set based on the determined protection level. In step S2000, the document requiring forgery protection, including the protection techniques of the determined protection level, is printed using the selected trusted printer. Then in step S2100 the method ends.

Although one exemplary embodiment of a document forgery protection printing method according to this invention has been described above with respect to Fig. 2, it should be appreciated that other exemplary embodiments of document forgery protection printing methods may be apparent to those of ordinary skill in the art. For example, in various exemplary embodiments of the document forgery protection printing method according to this invention, the information about the protection levels may be displayed prior to the print command being entered. In other various exemplary embodiments of the document forgery protection printing method invention of this invention, the information about the value of the document and the potential forgery of the document may also be collected prior to the print command being entered . In other various exemplary embodiments of the document forgery protection printing method according of this invention, the parameters of the selected trusted printer may be set prior to the print job being routed to the selected trusted printer.

While this invention has been described in conjunction with the various exemplary embodiments outlined above, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, the various exemplary embodiments of the invention, as set forth above, are intended

to be illustrative, not limiting. Various changes may be made without departing from the spirit and scope of the invention.

WHAT IS CLAIMED IS:

1. A document forgery protection printing method, comprising:

processing an image of a document;

determining forgery protection requirements for the document to be printed;

determining a protection level to be applied to the document based on the determined forgery protection requirements;

selecting a printer from a plurality of printers that can print the document; and

based on the determined protection level, printing at least one watermark on the document that corresponds to the determined protection level using the selected printer.

2. The method of claim 1, wherein determining the forgery protection requirements includes displaying information about forgery techniques.

3. The method of claim 2, wherein displaying information further includes displaying information about forgery techniques each protection level is able to at least one of detect and deter.

4. The method of claim 1, wherein determining the forgery protection requirements includes collecting information about the document.

5. The method of claim 1, wherein determining the protection level includes identifying at least one of a creator of the document, a person entering a command to print the document, and an image processor that processes the image of the document.

6. The method of claim 1, wherein determining the protection level includes reviewing contents of the document.

7. The method of claim 1, further comprising querying the plurality of printers to determine the protection level each printer can apply to the document.

8. The method of claim 1, further comprising setting printing parameters on the selected printer to apply the determined protection level to the document.

9. The method of claim 1, wherein determining the protection level includes at least one of assigning and selecting the protection level by at least one of a creator of the document and a person entering a command to print the document.

10. A document forgery protection printing system, comprising:

at least one server having a print management system and a policy that determines a forgery protection level for the document;

at least one image processor that processes an image of the document;

a plurality of printers, each printer able to print the document and able to apply at least one protection level to the document by printing at least one watermark on the document that corresponds to the determined protection level.

11. The document forgery protection printing system of claim 10, further comprising a display device, at least one of the server and one of the at least one image processors driving the display device to display information about forgery techniques.

12. The document forgery protection printing system of claim 11, wherein the displayed information includes information about forgery techniques each protection level is able to at least one of detect and deter.

13. The document forgery protection printing system of claim 10, wherein the policy determines the protection level for the document based on information collected from at least one of a creator of the document and a person entering a command to print the document.

14. The document forgery protection printing system of claim 10, wherein the policy determines the protection level based on at least one of a creator of the document, a person entering a command to print the document, and an image processor that processes the image of the document.

15. The document forgery protection printing system of claim 10, wherein the policy determines the protection level based on contents of the document.

16. The document forgery protection printing system of claim 10, wherein the policy determines the protection level based at least in part on a protection level assigned to the document.

17. The document forgery protection printing system of claim 10, wherein the server sets printing parameters for the selected printer selected to apply the determined protection level to the document.

ABSTRACT OF THE DISCLOSURE

A print management system includes a policy that determines a protection level for a document to be printed. The document is printed using forgery detection and deterrence technologies, such as fragile and robust watermarks, glyphs, and digital signatures, that are appropriate to the level of protection determined by the policy. A plurality of printers are managed by a print management system. Each printer can provide a range of protection technologies. The policy determines the protection technologies for the document to be printed and the print management system routes the print job to a printer that can apply the appropriate protections and sets the appropriate parameters in the printer. Copy evidence that can verify that a document is a forgery and/or tracing information that identifies the custodian(s) of the document and restrictions on copying of the document and use of the information in the document are included in the watermark that is printed with the document information. A document can be verified as an original or a forgery by inspecting the copy evidence and/or tracing information in the watermark.

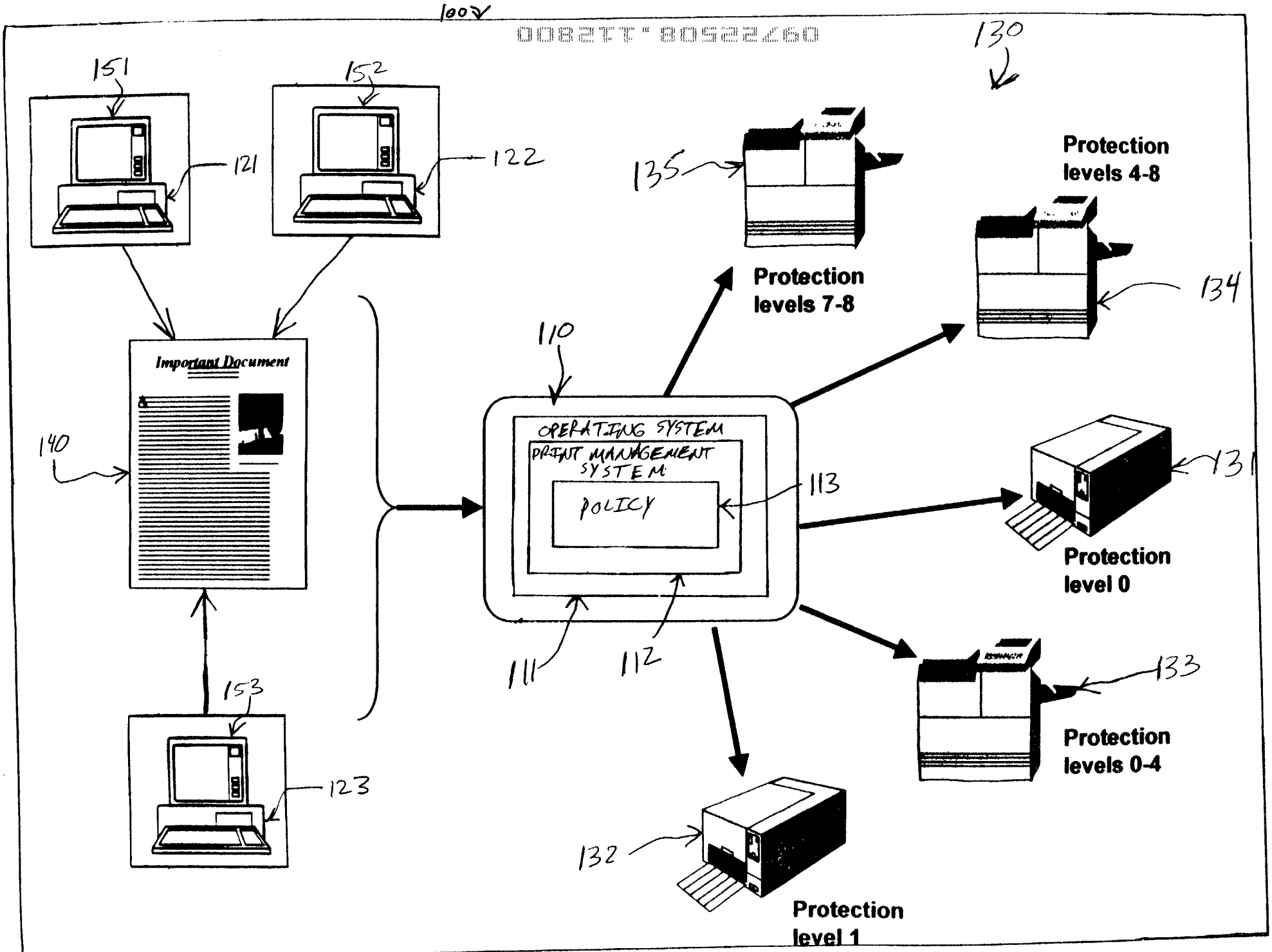
100
00827T "80522260
130
151
152
121
122
135
Protection levels 4-8
Protection levels 7-8
134
110
Important Document
140
OPERATING SYSTEM
PRINT MANAGEMENT SYSTEM
POLICY
113
131
Protection level 0
153
123
111
112
133
Protection levels 0-4
132
Protection level 1

FIG. 1

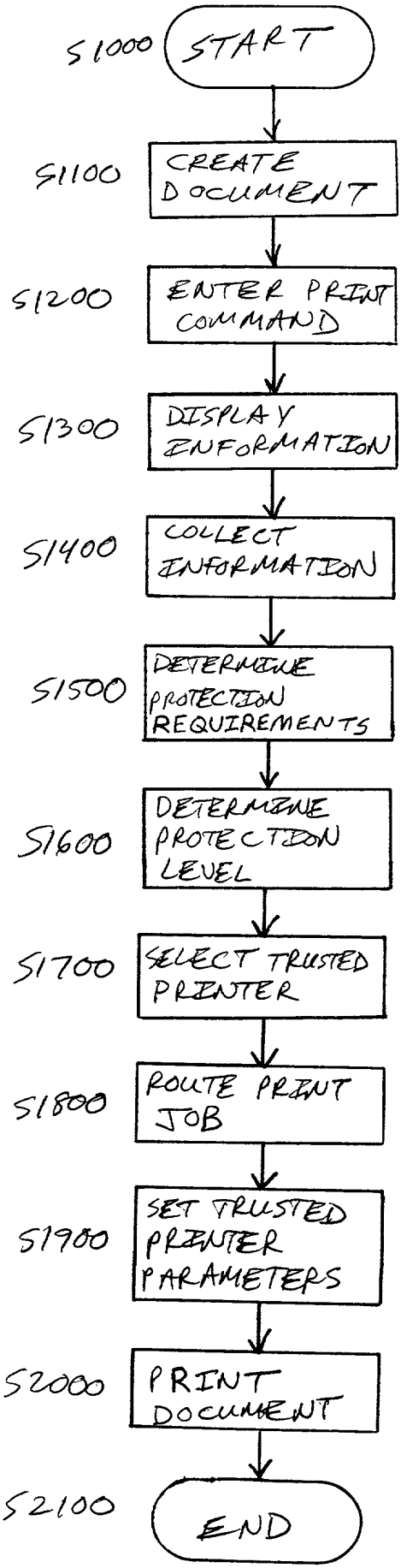
S1000
START
S1100
CREATE DOCUMENT
S1200
ENTER PRINT COMMAND
S1300
DISPLAY INFORMATION
S1400
COLLECT INFORMATION
S1500
DETERMINE PROTECTION REQUIREMENTS
S1600
DETERMINE PROTECTION LEVEL
S1700
SELECT TRUSTED PRINTER
S1800
ROUTE PRINT JOB
S1900
SET TRUSTED PRINTER PARAMETERS
S2000
PRINT DOCUMENT
S2100
END

FIG. 2

Docket No.: 104135

APPLICATION FOR UNITED STATES PATENT
DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name; that

I verily believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural inventors are named below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEMS AND METHODS FOR POLICY BASED PRINTING

described and claimed in the specification:

Check one

*a. ☒ attached hereto.

b. ☐ filed on _____ as Application No. _____ and amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, §1.56. Under Title 35, U.S. Code §119, the priority benefits of the following foreign application(s) and/or United States provisional application(s) filed by me or my legal representatives or assigns within one year prior to this application are hereby claimed:

NONE.

The following application(s) for patent or inventor's certificate on this invention were filed in countries foreign to the United States of America either (a) more than one year prior to this application, or (b) before the filing date of the above-named foreign priority application(s) and/or United States provisional application(s):

NONE.

I hereby appoint the following as my attorneys of record with full power of substitution and revocation to prosecute this application and to transact all business in the Patent Office:

**James A. Oliff, Reg. No. 27,075; William P. Berridge, Reg. No. 30,024;
Kirk M. Hudson, Reg. No. 27,562; Thomas J. Pardini, Reg. No. 30,411;
Edward P. Walker, Reg. No. 31,450; Robert A. Miller, Registration No. 32,771;
Mario A. Costantino, Registration No. 33,565; Caroline D. Dennison, Registration No. 34,494;
and John Beck, Reg. No. 22,833.**

ALL CORRESPONDENCE IN CONNECTION WITH THIS APPLICATION SHOULD BE SENT TO OLIFF & BERRIDGE, PLC, P.O. BOX 19928, ALEXANDRIA, VIRGINIA 22320, TELEPHONE (703) 836-6400.

I hereby declare that I have reviewed and understand the contents of this Declaration, and that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

1 ***Typewritten Full Name of First or Sole Inventor***

Teresa	F.	LUNT
Given Name	Middle Initial	Family Name

2 ****INVENTOR'S SIGNATURE:** Teresa F. Lunt 4-11-2000

3 ****DATE OF SIGNATURE:**

Month	Day	Year

Residence:	Palo Alto	CA	U.S.A.
	City	State or Province	Country
Citizenship:	United States		

Post Office Address:
(Insert complete mailing address, including country)

892 Bruce Drive

Palo Alto, CA 94303 USA

***This form may be executed only when attached to the specification (including claims) at the end thereof if Box a. is checked.**

****Note to Inventor: Please sign name exactly as it appears above and insert actual date of signing.**

IF THERE IS MORE THAN ONE INVENTOR USE PAGE 2 AND PLACE AN "X" HERE ☒

1 ***Typewritten Full Name of Second Joint Inventor (if any)***

Matthew	K.	FRANKLIN
Given Name	Middle Initial	Family Name

2 ****INVENTOR'S SIGNATURE:** Matthew K. Franklin

3 ****DATE OF SIGNATURE:**

April	11	2000
Month	Day	Year

Residence:

Palo Alto	CA	U.S.A.
City	State or Province	Country

Citizenship: United States

Post Office Address: (Insert complete mailing address, including country) 334 Grant Avenue
Palo Alto, CA 94306 U.S.A.

1 ***Typewritten Full Name of Third Joint Inventor (if any)***

Given Name	Middle Initial	Family Name

2 ****INVENTOR'S SIGNATURE:**

3 ****DATE OF SIGNATURE:**

Month	Day	Year

Residence:

City	State or Province	Country

Citizenship:

Post Office Address: (Insert complete mailing address, including country)

1 ***Typewritten Full Name of Fourth Joint Inventor (if any)***

Given Name	Middle Initial	Family Name

2 ****INVENTOR'S SIGNATURE:**

3 ****DATE OF SIGNATURE:**

Month	Day	Year

Residence:

City	State or Province	Country

Citizenship:

Post Office Address: (Insert complete mailing address, including country)

1 ***Typewritten Full Name of Fifth Joint Inventor (if any)***

Given Name	Middle Initial	Family Name

2 ****INVENTOR'S SIGNATURE:**

3 ****DATE OF SIGNATURE:**

Month	Day	Year

Residence:

City	State or Province	Country

Citizenship:

Post Office Address: (Insert complete mailing address, including country)

**Note to Inventors: Please sign name exactly as it appears and insert the actual date of signing.
This form may be executed only when attached to the first page of the Declaration and Power of Attorney form and the specification (including claims) of the application to which it pertains.